3/24/2025

แผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ

IT Disaster Recovery Plan (IT-DRP)

สารบัน

แผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ
IT Disaster Recovery Plan - (IT-DRP)

บทนำ

แผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ IT Disaster Recovery Plan -(IT-DRP) ฉบับนี้จัดทำขึ้นเพื่อให้งานเทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ สามารถนำไปใช้ในการปฏิบัติงานในสภาวะ วิกฤติ เช่น ภัยคุกคามทางไซเบอร์ การเกิดอัคคีภัย การเกิดอุทกภัย การก่อการร้าย ประท้วง จลาจล ที่จะส่งผลให้ระบบสารสนเทศที่ใช้ปฏิบัติงานหลักไม่สามารถให้บริการได้ โดยแผนฟื้นฟูระบบสาระสนเทศ ได้แนวทางการวิเคราะห์ความสำคัญของกระบวนการในภารกิจที่มีระบบสารสนเทศที่ใช้งานเป็นหลัก ซึ่งเมื่อมีการหยุดชะงักจะก่อให้เกิดผลกระทบต่อภาระหน้าที่ และฐานข้อมูลหลักของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เช่น ระบบฐานข้อมูลเพื่องานวิจัย ระบบสารสนเทศเพื่อการตัดสินใจ ระบบสารสนเทศบริการอาจารย์และนักศึกษา ระบบบริหารงานบุคคล และระบบต่าง ๆ ที่อยู่ในการกำกับดูแลของสำนักวิทยบริการและเทคโนโลยีสารสนเทศมาจัดทำแผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสามารถกลับมาดำเนินการได้ตามปกติหรือให้บริการได้ในสภาวะฉุกเฉินในระยะเวลาที่เหมาะสม ลดความความรุนแรงของเหตุการที่ เกิดขึ้นได้

วัตถุประสงค์

๑. จัดทำแผนฟื้นฟูระบบสาระสนเทศเพื่อนำไปปฏิบัติใช้เมื่อเกิดเหตุการณ์ภัยพิบัติที่อาจส่งผลกระทบต่อการ ปฏิบัติงานภายในสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

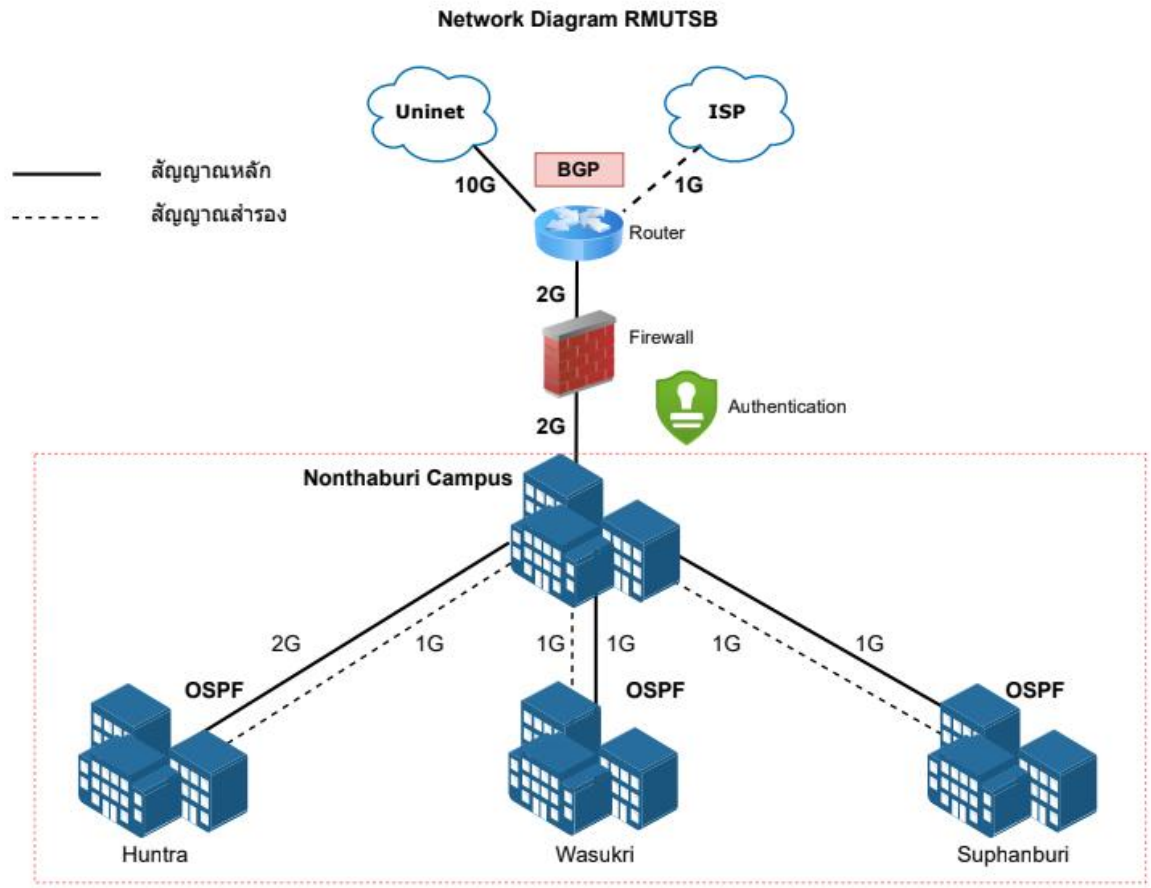
๒. เพื่อให้เจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศหรือผู้ที่เกี่ยวข้องทราบขั้นตอนการรับมือ

๓. เพื่อลดผลกระทบจากการหยุดชะงักในการให้บริการ

๔. กำหนดขั้นตอนการฟื้นฟูบริการระบบสารสนเทศ

ขอบเขต

แผนฟื้นฟูระบบสาระสนเทศ จะถูกนำมาใช้เมื่อมีการประสบเหตุการภัยพิบัติที่เกิดขึ้น เช่น อาคารสำนักงาน/ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้รับความเสียหาย ไฟไหม้ น้ำท่วม การก่อการประท้วง/จลาจล และภัยคุกคามทางไซเบอร์จนระบบหยุดชะงักไม่ สามารถใช้งานได้



รูปที่ ๑ ผังโครงสร้างระบบเครือข่ายมหาวิทยาลัยราชมงคลสุวรรณภูมิ

๑.Application Server และฐานข้อมูลภายในสำนักวิทยบริการและเทคโนโลยีสารสนเทศประกอบไปด้วยระบบต่าง ๆ ที่ใช้งาน ระบบสำคัญหลัก คือ การให้บริการอินเตอร์เน็ต ระบบให้บริการอาจารย์และนักศึกษา ระบบบริหารงานบุคลากร และระบบเว็บไซต์มหาวิทยาลัย

๒.ระบบเครือข่ายและอินเตอร์เน็ต สำหรับเชื่อมต่อกับภายนอกมีการตรวจสอบตัวตนผ่านระบบพิสูจน์ตัวตน และอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ เพื่อป้องกันการบุกรุก

๓.หน่วยงานที่เกี่ยวข้องหรือใช้งานระบบสารสนเทศหลัก จะประกอบไปด้วย คณะ/สำนักและกองต่างๆ ภายใต้มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

ลำดับความสำคัญของกระบวนการหลักและเป้าหมายการทำงาน

กระบวนการหลักที่ต้องให้ความสำคัญและจำเป็นต้องดำเนินให้บริการได้ และเป้าหมายระยะเวลาสูงสุดที่ยอมรับ ได้ในการยอมให้คอมพิวเตอร์ ระบบเครือข่าย หรือ แอปพลิเคชันหยุดทำงานได้ หลังเกิดเหตุขัดข้อง คือ ๒ วัน และปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้คือ ๑ วัน

กระบวนการหลัก	รายละเอียด	ระดับความสำคัญ	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Maximum Tolerable Period of Disruption (MTPD)
การให้บริการระบบอินเตอร์เน็ต	ระบบเครือข่ายอินเตอร์เน็ต ระบบเครือข่ายเชื่อมโยงศูนย์พื้นที่ ระบบแม่ข่ายบริการสารสนเทศ - ระบบโดเมน DNS - ระบบแจกเลขไอพี (DHCP) - ระบบบัญชีผู้ใช้ (AD) - ระบบยืนยันตัวตน - ระบบจัดเก็บ LOG	๑	๔ ชั่วโมง	๑ วัน	๒ วัน
การป้องกันภัยคุกคามทางไซเบอร์	ระบบป้องกันภัยคุกคามทางไซเบอร์ - Firewall/IPS/WAF - EDR - Antivirus	๒	๔ ชั่วโมง	๑ วัน	๒ วัน
การให้บริการระบบสารสนเทศสำหรับอาจารย์และนักศึกษา	ระบบสารสนเทศงานบริการอาจารย์และนักศึกษา - ระบบใบคำร้อง RMS - ระบบรับสมัครนักศึกษา - ระบบ Email - ระบบห้องสมุดอัตโนมัติ - ระบบศิษย์เก่า - ระบบทะเบียนและประมวลผล - ระบบคลังหน่วยกิต - ระบบบัตรนักศึกษา - ระบบ Digital Transcript	๓	๑ วัน	๓ ชั่วโมง	๒ วัน

	- ระบบพิธีรับปริญญาบัตร - ระบบบริการงานทะเบียน - ระบบสหกิจศึกษา				
ระบบสารสนเทศงานบริหารงานบุคคล	ระบบสารสนเทศงานบริหารงานบุคคล - ระบบ HRD - ระบบ HRS - ระบบลางาน (lanoline) - ระบบสลิปเงินเดือน - ระบบ E-profile - ระบบบันทึกเวลาทำงาน - ระบบเบิกสวัสดิการ - ระบบบันทึกภาระงาน	๔	๑ วัน	๓ ชั่วโมง	๒ วัน
การให้บริการระบบและเว็บไซต์มหาวิทยาลัย	ระบบสารสนเทศมหาวิทยาลัย - เว็บไซต์มหาวิทยาลัย/คณะ/หน่วยงาน - ระบบสารบรรณอิเล็กทรอนิกส์ - ระบบครุภัณฑ์ - ระบบแจ้งซ่อมออนไลน์ - ระบบจองห้องประชุม - ระบบ Webometric - ระบบช่วยการบริหารและตัดสินใจ (Dashboard, MOU) - ระบบร้องเรียน - เว็บไซต์สภาวิชาการ	๕	๑ วัน	๑ วัน	๒ วัน
ระบบงานวิจัย	ระบบสารสนเทศเพื่องานวิจัย - ระบบฐานข้อมูลงานวิจัย	๖	๑ วัน	๑ วัน	๒ วัน

การดำเนินการตรวจสอบ/แจ้งเตือนระบบสารสนเทศ	ระบบตรวจสอบ/แจ้งเตือนระบบสารสนเทศ - KUMA - Cacti - Nagios - Grafana - Zabbix - Discord - Line - Google	๗	๑ วัน	๑ วัน	๒ วัน

ตารางที่ ๑ ลำดับความสำคัญระบบสารสนเทศ

ความหมายของคำสำคัญที่ปรากฏในตารางข้างต้นอธิบายได้ดังต่อไปนี้

- Recovery Time Objective (RTO) - period of time following an incident within which the business activity must be resumed
- Recovery Point Objective (RPO) - point to which information used by an activity must be restored to enable the activity to operate on resumption. Also referred to as Minimum Data Loss
- Maximum Tolerable Period of Disruption (MTPD) -The Maximum Time Period of Disruption (MTPD) represents the estimated or predefined maximum duration that an organization's critical business services or operations can sustain a disruption before it reaches a point of critical impact or unacceptable consequences.

มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ได้เตรียมระบบสำรองการฟื้นฟูระบบแบบ Warm Site โดยจัดสถานที่สำรอง Warm Site ไว้ที่ Data center สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ศูนย์นนทบุรี ชั้น ๓ เมื่อมีเหตุการณ์อุบัติภัยหรือ Server ล่ม มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิจะทำการขึ้นระบบสำรองโดยใช้ข้อมูลที่สำรองล่าสุด ตามข้อกำหนดที่ได้ตกลงไว้ภายในระยะเวลาที่มหาวิทยาลัยยอมรับได้

การกำหนดไซต์สำรอง (Disaster Recovery Site)

๑. Hot Site ระบบสำรองจะสามารถใช้งานได้เหมือนระบบหลัก รวมทั้งข้อมูลต่าง ๆ จะถูกเก็บทั้งสองแห่ง ลักษณะเหมือนเป็น Mirror Site หากเกิดภัยพิบัติหรือระบบล่ม สามารถขึ้นระบบสำรองให้ทำงานทดแทนได้เกือบจะในทันทีทันใด แต่มีข้อเสียคือ ใช้งบประมาณในการดำเนินการสูง

๒. Warm Site ระบบสำรองที่สามารถทำงานได้เหมือนระบบหลัก แต่ในส่วนของข้อมูลนั้นจะต้องนำข้อมูลที่ได้สำรอง (Backup) ไว้จากระบบหลักมา Restore จึงจะสามารถใช้งานได้ แต่อาจมีข้อมูลบางส่วนที่ยังไม่ได้ถูกสำรองไว้สูญหายบ้าง อีกทั้งต้องใช้เวลาในการติดตั้งฐานข้อมูลช่วงเวลาหนึ่งก่อนที่ระบบจะสามารถทำงานต่อไปได้

๓. Cold Site เป็นการจัดเตรียมโครงสร้างพื้นฐานต่าง ๆ ไว้ก่อนแล้ว อาทิเช่น ระบบเครื่องปรับอากาศ ระบบเครือข่าย ระบบโทรศัพท์ เมื่อเกิดภัยพิบัติหรือระบบล่ม จะต้องจัดหาเครื่องคอมพิวเตอร์มาติดตั้งจึงจะสามารถทำงานระบบต่อได้ แต่ข้อเสียคือ ต้องใช้เวลาในการติดตั้งระยะหนึ่งกว่าระบบจะทำงานได้ตามปกติ

๔. Standby Site เป็นการจัดหาพื้นที่เตรียมไว้ แต่ไม่ได้ดำเนินการใด ๆ เกี่ยวกับระบบคอมพิวเตอร์

๕. Nothing คือการไม่ได้จัดเตรียมสิ่งใดไว้สำหรับระบบสำรองเลย

เกณฑ์การประเมินระดับเหตุการณ์

ระดับเหตุการณ์	คำอธิบาย
๑	เกิดเหตุการณ์ไม่ปกติ เช่น การโจมตีทางไซเบอร์ ภัยจากการชุมนุมประท้วง น้ำท่วม ไฟไหม้บริเวณข้างเคียง แต่ระบบสำคัญยังใช้งานได้
๒	เกิดเหตุการณ์ที่ส่งผลให้ระบบสำคัญไม่สามารถใช้งานได้เป็นระยะเวลานาน เช่น กระแสไฟฟ้าแรงสูงขัดข้อง เกิดภัยคุกคามทางไซเบอร์ ซึ่งต้องใช้เวลานานในการแก้ไข แต่ยังสามารถเข้าออกศูนย์คอมพิวเตอร์หลักได้
๓	เกิดเหตุการที่มีความรุนแรงมากที่สุดเช่น อัคคีภัย อุทกภัย เสียหายต่อตัวอาคารหรือ ศูนย์คอมพิวเตอร์หลักและระบบสำคัญ เป็นเหตุให้ไม่สามารถให้บริการระบบเทคโนโลยีสารสนเทศได้เป็นเวลานาน

ตารางที่ ๒ เกณฑ์การประเมินระดับเหตุการณ์

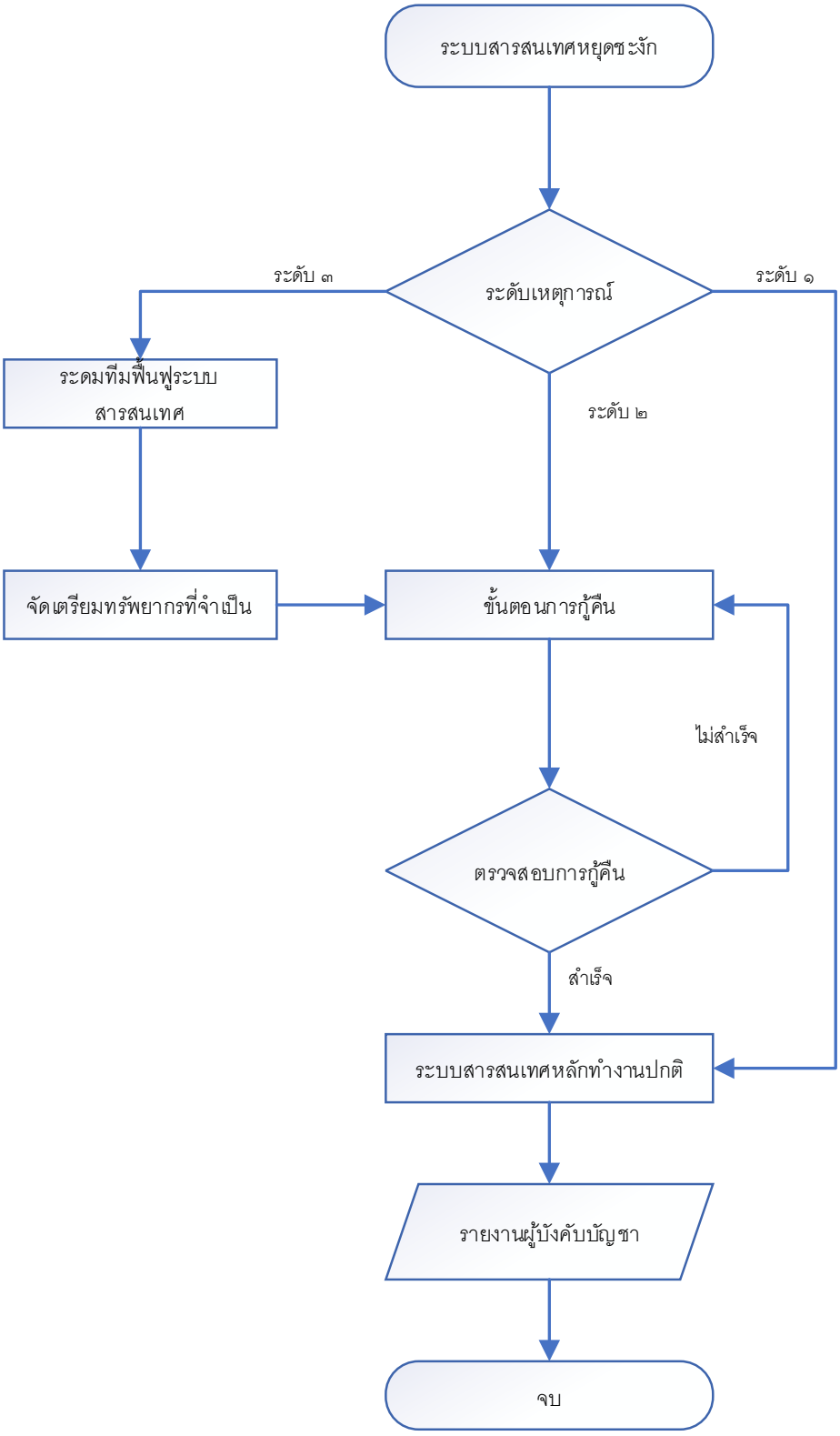
แนวทางการปฏิบัติการตามระดับเหตุการณ์

ระดับเหตุการณ์	๑ เหตุการณ์ทั่วไป (Minor)
ผลกระทบ	เกิดเหตุการณ์ไม่ปกติ เช่น การโจมตีทางไซเบอร์ จากการชุมนุมประท้วง น้ำท่วม ไฟไหม้ บริเวณข้างเคียง แต่ระบบสำคัญยังใช้งานได้
แนวทางปฏิบัติ	แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree ประเมินสถานการณ์เฝ้าระวัง สำรองข้อมูลระบบสำคัญ
ระดับเหตุการณ์	๒ เหตุการณ์รุนแรง (Major)
ผลกระทบ	เกิดเหตุการณ์ที่ส่งผลให้ระบบสำคัญไม่สามารถใช้งานได้เป็นระยะ เวลานาน เช่น กระแสไฟฟ้าแรงสูงขัดข้อง มีเกิดภัยคุกคามทางไซเบอร์ ซึ่งต้องใช้เวลานานในการแก้ไขแต่ยังสามารถเข้าออกศูนย์คอมพิวเตอร์หลักได้
แนวทางปฏิบัติ	แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree เข้าตรวจปัญหา/ประเมินผลความเสียหายและสถานการณ์ จัดเตรียมคอมพิวเตอร์ชั่วคราวที่สามารถเชื่อมต่ออินเตอร์เน็ตผ่านระบบ มือถือได้ ฟื้นฟูข้อมูลระบบที่เกิดการหยุดชะงัก ตรวจสอบการใช้งานระบบ
ระดับเหตุการณ์	๓ เหตุการณ์หายนะ (Crisis)
ผลกระทบ	เกิดเหตุการที่มีความรุนแรงมากที่สุดเช่น ภัยคุกคามทางไซเบอร์ อัคคีภัย อุทกภัย เสียหายต่อตัว อาคารหรือศูนย์คอมพิวเตอร์หลักและระบบสำคัญเป็นเหตุให้ไม่สามารถ ให้บริการระบบเทคโนโลยีสารสนเทศได้เป็น เวลานาน

แนวทางปฏิบัติ	แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree เข้าตรวจปัญหา/ประเมินผลความเสียหายและสถานการณ์ จัดเตรียมคอมพิวเตอร์ชั่วคราวที่สามารถเชื่อมต่ออินเตอร์เน็ต ผ่านระบบมือถือได้ เตรียมทีมฟื้นฟูระบบ ฟื้นฟูระบบสารสนเทศทั้งหมด ทดสอบการใช้งานระบบ ประสานงานหน่วยงานต่างๆ เพื่อใช้ระบบงานสำรอง

ตารางที่ ๓ แนวทางปฏิบัติตามระดับเหตุการณ์

กระบวนการฟื้นฟู



รูปที่ ๒ แผนผังกระบวนการฟื้นฟู

ทีมฟื้นฟู

หัวหน้าทีมฟื้นฟูระบบ จะต้องทำการติดต่อลูกทีมทั้งหมด ตามภาคผนวก ข. โดยจะต้องแจ้งสถานการณ์ที่เกิดขึ้นให้ลูกทีมได้รับทราบ และขอให้ไป รวมตัวกันที่สถานที่รวมพลตามที่อยู่ดังนี้

ที่อยู่ : สำนักงานอธิการบดี มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ศูนย์พระนครศรีอยุธยา หันตรา เลขที่ ๖๐ หมู่ ๓ ถ.สายเอเชีย (กรุงเทพฯ - นครสวรรค์) ต.หันตรา อ.พระนครศรีอยุธยา จ. พระนครศรีอยุธยา ๑๓๐๐๐

โทรศัพท์ : ๐๓๕-๗๐๙๑๐๓

โทรสาร : ๐๓๕-๗๐๙๐๘๓

กรณีที่สถานที่รวมพลในข้างต้นไม่สามารถเข้าถึงได้ หัวหน้าทีมฟื้นฟูระบบ จะต้องขอให้ลูกทีมไป รวมตัวกัน ณ สถานที่ แห่งที่ ๒ ตามที่อยู่ดังต่อไปนี้

ที่อยู่ : มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ศูนย์พระนครศรีอยุธยา วาสุกรี เลขที่ ๑๙ ถ. อู่ทอง ต. ท่าวาสุกรี อ. พระนครศรีอยุธยา จ. พระนครศรีอยุธยา ๑๓๐๐๐

โทรศัพท์ : ๐๓๕-๓๒๔๑๘๐

โทรสาร : ๐๓๕-๒๕๒๓๙๓

บทบาท และหน้าที่ความรับผิดชอบ

ลำดับที่	ชื่อ	บทบาท และหน้าที่รับผิดชอบ
๑	**หัวหน้าทีมฟื้นฟูระบบ** - หัวหน้างานเทคโนโลยีสารสนเทศ	o ประเมินสถานการณ์ที่เกิดขึ้นว่ามีผลกระทบและความรุนแรงในระดับใด o ระดมลูกทีมทั้งหมดเพื่อลงพื้นที่ปฏิบัติการประสานงาน และสั่งการให้ลูกทีมร่วมกัน ดำเนินการแก้ไขปัญหาที่พบ o รายงานสถานการณ์การฟื้นฟูระบบให้หน่วยติดตามสถานการณ์ ประธานคณะทำงานและคณะทำงานได้รับทราบอย่างเป็นระยะๆ o ประสานงานกับฝ่ายอาคารสถานที่ และฝ่าย รปภ. เพื่อขอให้ช่วยดำเนินการในเรื่องต่างๆ อาทิ ตรวจสอบระบบไฟฟ้า ระบบโทรศัพท์ระบบปรับอากาศ การรักษาความปลอดภัยหรืออื่นๆ ที่เกี่ยวข้อง o สั่งการให้ลูกทีมตรวจสอบและเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศต่างๆ ในศูนย์พื้นที่สำรอง o จัดทำรายงาน ภายหลังสถานการณ์สิ้นสุดลง

๒	**ทีมติดตั้งเซิร์ฟเวอร์และเครือข่าย** - นายจตุพร ระเวงจิตร - นายพันธฤทธิ์ พุ่มจำปา - นายสิริพงษ์ พิทักษ์สุข - นายณัฐวัฒน์ เขาแก้ว - นายสุวิชัย แช่มชื่น	o สำรวจและประเมินความเสียหายของฮาร์ดแวร์อุปกรณ์ ข้อมูลและ/หรือซอฟต์แวร์ต่างๆ ของระบบที่เกิดความเสียหายและจำเป็นต้องแก้ไขหรือติดตั้งกลับคืน o กำหนดรายการของฮาร์ดแวร์ อุปกรณ์ ข้อมูลและ/หรือซอฟต์แวร์ต่างๆ ที่จำเป็นต้องใช้ในการฟื้นฟู o แจ้งรายการฮาร์ดแวร์หรืออุปกรณ์ที่ต้องการพร้อมทั้งคุณลักษณะให้ทีมการจัดการทั่วไปช่วยดำเนินการจัดหาให้ o ติดตั้งฮาร์ดแวร์ อุปกรณ์ และ/หรือซอฟต์แวร์ที่เกี่ยวข้องกับระบบ โดยติดตั้งให้เหมือนเดิมหรือใกล้เคียงกับระบบเดิมให้มากที่สุด o นำข้อมูลล่าสุดที่สำรองเก็บไว้มาทำการติดตั้งกลับคืนตามความจำเป็น
๓	**ทีมติดตั้งแอพพลิเคชันและฐานข้อมูล** - นายศรัณพงษ์ ศรีพูน - นายณบุรินท์ สุภีวี - นายนฤทธิ์ แสงเปี่ยม - นายฐิตินันท์ ภู่พันธ์	o ติดตั้งและปรับแต่ง Application ให้เหมือนระบบเดิมมากที่สุด o ทดสอบฟังก์ชั่นการทำงานต่างๆ ของระบบเพื่อดูว่าสามารถใช้งานได้ครบถ้วนหรือไม่ o นำข้อมูลล่าสุด (ของฐานข้อมูล) ที่สำรองเก็บไว้มาทำการติดตั้งกลับคืนตามความจำเป็น o พยายามฟื้นฟูข้อมูลของระบบ ให้กลับไปสู่จุดเวลาที่เกิดเหตุหยุดชะงักขึ้น o ตรวจสอบดูความถูกต้องของข้อมูลที่ทำการติดตั้งกลับคืนนั้นเท่าที่ทำได้ o ทดสอบระบบร่วมกับผู้ใช้งาน

ตารางที่ ๔ บทบาท หน้าที่ ทีมฟื้นฟู

ในการดำเนินการฟื้นฟูระบบสารสนเทศจำเป็นต้องอาศัยการทำงานของแผนฟื้นฟูระบบสารสนเทศฉบับอื่น เช่น กรณีของบริการระบบสารสนเทศ ที่จำเป็นต้องอาศัยการทำงานของระบบไฟฟ้าหากระบบไฟฟ้าเกิดการขัดข้อง จะทำให้บริการระบบสารสนเทศไม่สามารถให้บริการได้ ดังนั้นบริการระบบสารสนเทศจึงต้องอาศัยแผนการแก้ไขระบบไฟฟ้าที่ขัดข้อง เพื่อแก้ไขกระแสไฟฟ้าให้กลับ คืนมาให้บริการได้ตามปกติ จากนั้นการทำงานของแผนฟื้นฟูบริการระบบสารสนเทศฉบับนี้จึงจะสามารถดำเนินต่อไปได้

ชื่อเอกสาร	รายละเอียดเอกสาร	ผู้รับผิดชอบ
แผนบริหารความต่อเนื่องในภาวะวิกฤตด้านเทคโนโลยีสารสนเทศ	การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCP)	สวส.
แผนรับมือภัยคุกคามทางไซเบอร์	แผนรับมือภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ (IR Plan)	สวส.
แผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan)	แผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan)	สวส.
แผนการสื่อสารในภาวะวิกฤตด้านเทคโนโลยีสารสนเทศ	แผนการสื่อสารในภาวะวิกฤตด้านเทคโนโลยีสารสนเทศ (Crisis Communication Management)	สวส.
แผนการแก้ไขระบบไฟฟ้าขัดข้อง		กองกลาง

ตารางที่ ๕ แผนด้านอื่นๆที่เกี่ยวข้อง

ในการฟื้นฟูระบบสารสนเทศจะต้องอาศัยการทำงานของอุปกรณ์ ต่าง ๆ ในสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เช่น เครื่องปรับอากาศ เครื่องสำรองไฟ ฯลฯ กรณีที่อุปกรณ์เหล่านี้เกิดความเสียหายทางกายภาพ ทีมฟื้นฟูบริการจำเป็นต้องอาศัยผู้ให้บริการภายนอกตามที่ปรากฏในตารางด้านล่าง นำอุปกรณ์มาเปลี่ยนทดแทนกรณี ที่เกิดความเสียหาย

หน่วยงาน		
ชื่อ/บริษัท	รายละเอียด/หน้าที่รับผิดชอบ	หมายเลขติดต่อ
สำนักเทคโนโลยีสารสนเทศและดิจิทัล (Uninet)	ผู้ให้บริการเชื่อมต่อระบบเครือข่าย	๐๒๒๓๒ ๔๐๐๐
Torque IT Co., Ltd.	MA, PM อุปกรณ์ Firewall SLA ตามสัญญา	๐๒-๐๐๒๐๙๖๕
บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด	ผู้ให้บริการเชื่อมต่อระบบเครือข่ายสำรอง SLA ตามสัญญา	๐๒-๒๕๗๒๗๐๐
บริษัท คอมเซิร์ฟ สยาม จำกัด	MA, PM, ห้อง DATA CENTER SLA ตามสัญญา	๐๒-๘๗๘๕๕๙๙
กองกลาง	ระบบไฟฟ้า	

ตารางที่ ๖ หน่วยงานที่เกี่ยวข้อง

ความต้องการด้านทรัพยากรในการฟื้นฟูบริการระบบสารสนเทศ

ทรัพยากรที่ต้องใช้	จำนวน
DATA Center	๑
อุปกรณ์กระจายสัญญาณ - layer ๓ - Fiber Channels	๒
เครื่องคอมพิวเตอร์แม่ข่าย - ๔๘ CPU ๓.๐ Ghz. - ๓๖๘ Gb RAM - SSD Disk ๕๐๐ Gb	๕
ระบบจัดเก็บข้อมูลกลาง - ๑๐๐ TB	๑
ระบบจัดเก็บข้อมูลกลาง สำหรับสำรองข้อมูล - ๖๐ TB	๑
Windows server ๒๐๒๒ (License)	๕
Hyper-V and Cluster	๔
Veem backup & replication enterprise	๑
Ssl VPN License	๑๐
SQL Server ๒๐๑๙ (License)	๒
Link Internet	๑ GB
Back UP SITE	๑

ตารางที่ ๗ ความต้องการด้านทรัพยากรสารสนเทศ

Checklist การฟื้นฟูระบบ

งานที่ต้องทำ		อ้างอิงขั้นตอนปฏิบัติ	ระยะเวลาที่ใช้ในการดำเนินการ	ระยะเวลาที่ทำได้จริง	ลายมือชื่อของผู้ดำเนินการ
การเตรียมความพร้อมของระบบสำรอง					
๑	ทีมฟื้นฟูบริการ ตรวจสอบความพร้อมใช้ของ ระบบเครือข่ายที่ไซต์สำรอง และดำเนินการตามที่เห็นสมควร เพื่อให้ระบบเครือข่ายพร้อมที่จะใช้งานได้				
๒	ทีมฟื้นฟูบริการ และ/หรือ ผู้ให้บริการภายนอก ร่วมกันจัดเตรียมระบบสำรองให้พร้อมใช้งาน โดยดำเนินการดังนี้ ● ดำเนินการ Restore ข้อมูลที่ได้ทำการสำรองไว้ลงไปยังระบบสำรองตามความจำเป็นแล้วแต่กรณี ● เชื่อมโยงและเปิดใช้ระบบสำรอง ● ทดสอบใช้งานระบบสำรองตามฟังชันที่สำคัญ ๆ ● กรณีที่ระบบสำรองมีปัญหา ให้ร่วมกันพิจารณาปัญหา กำหนดแนวทาง และดำเนินการแก้ไขจนกระทั่งแล้วเสร็จ				
การทดสอบใช้ระบบสำรองโดยผู้ใช้งาน					
๓	ทีมฟื้นฟูบริการ แจ้งให้ผู้ใช้งานดำเนินการ ทดสอบระบบสำรอง				
๔	ผู้ใช้งาน ยืนยันว่าระบบสามารถทำงานได้ ตามปกติหรือไม่ กลับมายังทีมฟื้นฟู				
๕	กรณีที่ระบบสำรอง**ไม่สามารถทำงานได้ตาม ปกติ** ทีมฟื้นฟูบริการ และ/หรือ ผู้ให้บริการภายนอก ร่วมกันพิจารณาปัญหา กำหนดแนวทาง และดำเนินการแก้ไขจนกระทั่งแล้ว เสร็จ				
การรายงานผลการฟื้นฟูระบบ					
๖	ทีมฟื้นฟูบริการ รายงานผลการกู้ระบบโดยใช้ ระบบสำรองให้ หัวหน้าทีมฟื้นฟูระบบ ได้รับ ทราบ				
๗	หัวหน้าทีมฟื้นฟูระบบ รายงานผลการแก้ไข ระบบให้คณะกรรมการบริหาร เพื่อรายงาน คณะกรรมการ ให้รับทราบต่อไป				

การสำรองข้อมูลบนระบบสำรอง					
๘	ในระหว่างที่ยังใช้งานระบบสำรองเพื่อ ปฏิบัติงาน ทีมฟื้นฟูบริการดำเนินการสำรอง ข้อมูลบนระบบสำรองด้วยความถี่เดียวกับ ความถี่ในการสำรองข้อมูลของระบบหลัก				

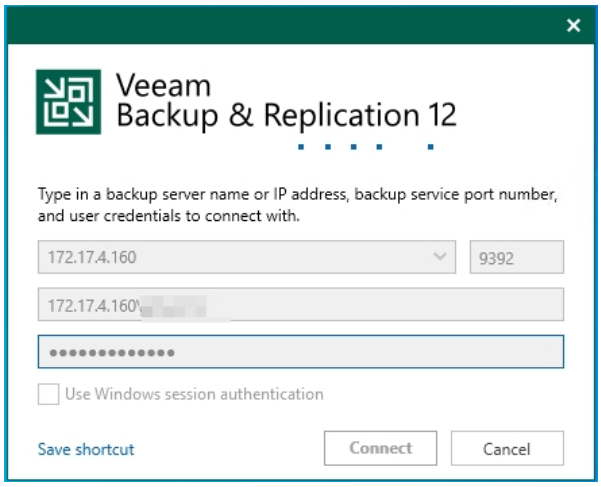
ตารางที่ ๘ checklist การฟื้นฟูระบบ

ภาคผนวก

ก.ขั้นตอนการกู้คืน HyperV โดย Veem

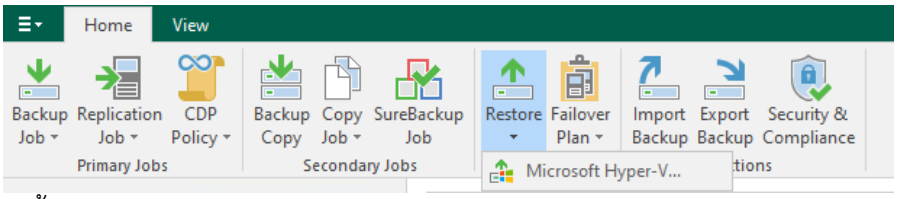
๑. เข้าสู่ Veeam Backup & Replication Console

- เปิด Veeam Backup & Replication console และเข้าสู่ระบบด้วยบัญชีผู้ใช้ที่มีสิทธิ์ในการเข้าถึง



๒. เลือกงานที่ต้องการฟื้นฟู

- ไปที่แท็บ "Home" และคลิกที่ "Restore" หรือ "Restore wizard"
- เลือก "Microsoft Hyper-V" เพื่อเลือกตัวเลือกที่เกี่ยวข้องกับการฟื้นฟูระบบ Hyper-V



๓. เลือกประเภทการฟื้นฟู

- คุณจะต้องเลือกประเภทการฟื้นฟูที่ต้องการ:

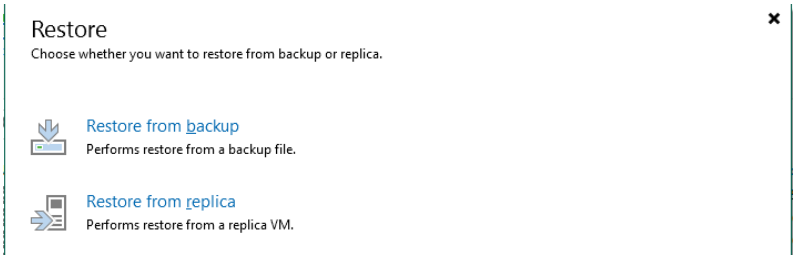
ก. Full VM Restore: การฟื้นฟูทั้งเครื่อง (Virtual Machine)

ข. VM files restore: ฟื้นฟูไฟล์ของ VM ที่หายไปหรือเสียหาย

ค. Instant VM Recovery: การฟื้นฟูและเรียกใช้ VM โดยตรงจากการสำรองข้อมูลโดยไม่ต้องรอให้การฟื้นฟูเสร็จสิ้น

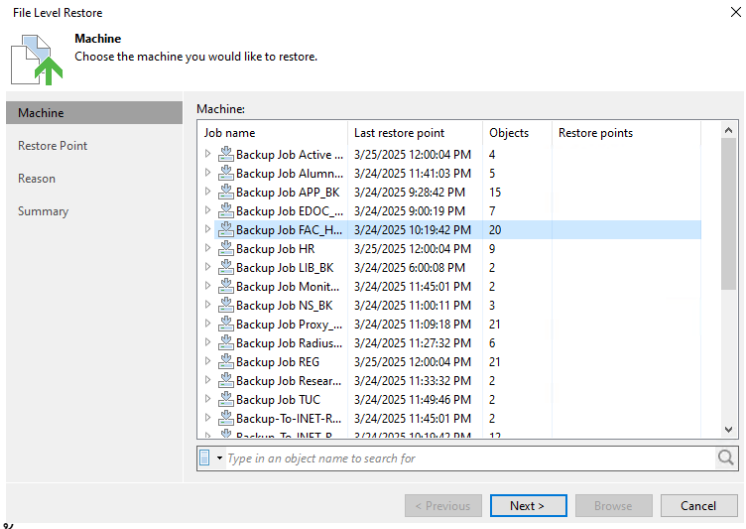
๔. เลือกสำเนาสำรอง (Backup Source)

- เลือกสำเนาสำรองที่คุณต้องการฟื้นฟูจากนั้นเลือกจุดเวลาที่ต้องการฟื้นฟูจาก Backup หรือ Replication



๕. เลือก VM ที่ต้องการฟื้นฟู

- หลังจากที่เลือกแหล่งข้อมูลสำรอง (Backup Source) แล้ว คุณจะเห็นรายการของ Virtual Machines (VMs) ที่มีการสำรองข้อมูล
- เลือก VM ที่คุณต้องการฟื้นฟู



๖. กำหนดพารามิเตอร์การฟื้นฟู

- กำหนดว่าคุณต้องการฟื้นฟู VM ไปยังสถานที่เดิม (Original Location) หรือสถานที่ใหม่ (Alternative Location)
- คุณอาจต้องเลือก Host, Cluster, หรือ Datastore ที่คุณต้องการให้เครื่องไปยัง VM ฟื้นฟู

๗. เลือกวิธีการฟื้นฟู

- Restore to the original location: ฟื้นฟู VM ไปยังสถานที่เดิม
- Restore to a new location: ฟื้นฟู VM ไปยังสถานที่ใหม่
- Restore to a new VM: ฟื้นฟูเป็นเครื่อง VM ใหม่

๘. กำหนดการตั้งค่าเพิ่มเติม

- คุณสามารถตั้งค่าการฟื้นฟูเพิ่มเติม เช่น การเปลี่ยนแปลงข้อมูลใน VM (เช่น IP, Network Adapter) หากต้องการ

๙. เริ่มการฟื้นฟู

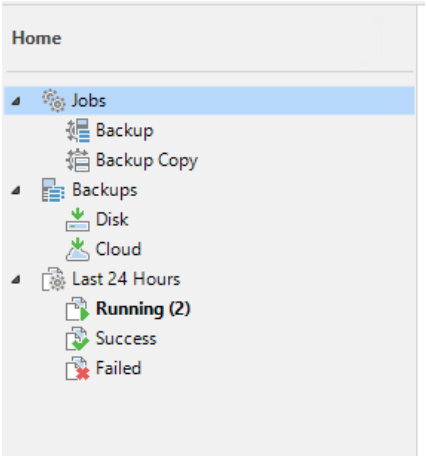
- ตรวจสอบการตั้งค่าทั้งหมด แล้วคลิกที่ "Finish" เพื่อเริ่มการฟื้นฟู
- Veeam จะเริ่มทำการฟื้นฟูตามที่คุณเลือกไว้

๑๐. ติดตามสถานะการฟื้นฟู

- คุณสามารถติดตามสถานะการฟื้นฟูในแท็บ "History" หรือในส่วน "Jobs" ของ Veeam Backup & Replication console

๑๑. ตรวจสอบผลการฟื้นฟู

- เมื่อการฟื้นฟูเสร็จสิ้น, ตรวจสอบว่า VM ที่ฟื้นฟูทำงานได้อย่างถูกต้อง



ข.รายชื่อผู้ติดต่อทีมฟื้นฟูระบบ

ชื่อ นาม-สกุล	ตำแหน่ง	การติดต่อ
นายณัฐวัฒน์ เขาแก้ว	นักวิชาการคอมพิวเตอร์ชำนาญการ	nattawat.k@rmutsb.ac.th
นายจตุพร ระเวงจิตร	นักวิชาการคอมพิวเตอร์ชำนาญการ	Jatuporn.r@rmutsb.ac.th
นายวิทยา ปานเพชร	นักวิชาการคอมพิวเตอร์ชำนาญการ	Witthaya.p@rmutsb.ac.th
นายฐิตินันท์ ภู่พันธ์	นักวิชาการคอมพิวเตอร์ชำนาญการ	thitinan.p@rmutsb.ac.th
นายสิริพงษ์ เกียรติพิทักษ์สุข	นักวิชาการคอมพิวเตอร์ชำนาญการ	Siripong.k@rmutsb.ac.th
นายพันธฤทธิ์ พุ่มจำปา	นักวิชาการคอมพิวเตอร์ชำนาญการ	Phanthalit.p@rmutsb.ac.th
นางสาวณชนก เรืองสะอาด	นักวิชาการคอมพิวเตอร์	nachanok.r@rmutsb.ac.th
นายศรัณย์พงษ์ ศรีพูน	นักวิชาการคอมพิวเตอร์	saranphong.s@rmutsb.ac.th
นายนฤทธิ์ แสงเปี่ยม	นักวิชาการคอมพิวเตอร์	narit.s@rmutsb.ac.th
นายสุวิชัย แช่มชื่น	นักวิชาการคอมพิวเตอร์	suwichai.c@rmutsb.ac.th
นายบุรินท์ สุภีวี	นักวิชาการคอมพิวเตอร์	burin.su@rmutsb.ac.th
นายจิรวัฒน์ พงษ์วิเชียร	นักวิชาการคอมพิวเตอร์	Jirawat.p@rmutsb.ac.th
นายประภาส บุญเสมอกุล	นักวิชาการคอมพิวเตอร์	prapard.b@rmutsb.ac.th